Security for your collaborative software

csoonline.com/article/3126586/security/security-for-your-collaborative-software.html

John Brandon

There's a gaping hole in your security infrastructure right now. The front door is open, the side window is ajar, and there's an open safe with a neon sign saying "steal my data" in flashing lights. While you might have locked down the network used for this software, instituted strict usage policies, and insist on having users stick to complex passwords, the data is leaking.

Collaborative apps like Slack and Convo are like a sieve at some larger companies, but no one quite knows what to do about it. The apps let users share documents, business plans, financials, and many other files, but one reason it's such a security risk is that we tend to use these glorified chat tools all day, everyday.

As security experts explained to CSO, the file-sharing features in particular have created a gaping hole that few have plugged.

"The convenience of file sharing could easily transform into a data breach if employees are not careful about what files they are dropping into private or public channels, especially if there is no security software in place to stop them from sharing sensitive data," says Roman Foeckl, CEO and founder of global endpoint security provider, CoSoSys.

Foeckl says Slack, with more than 3 million daily users and total dominance in the market (77 percent of Fortune 500 companies now use it), is prone to leaks when employees don't think about taking secure files and sharing them in a way that could create a serious problem.

"The insider threat is very real with Slack, whether it is in the form of an employee accidentally sharing customer database, intentional disclosure of company business plans, or Social Security numbers being shared to the public cloud," he says.

Mike McCamon, president of SpiderOak, a secure file-sharing and backup tool, went several steps further in questioning collaborative software security. He compares these apps to the USB thumbdrive a user carries out of the building that contains company financials. And, he says he has heard of some companies starting to question the use of these apps.

The biggest issue, of course, is that few of the collaborative chat apps use end-to-end encryption for the user activity. Hackers could sniff out a file transfer from one of these Web-based apps that rely on the browser as the main security platform.

"There is a long history of browser, plugins, and extension vulnerabilities," he says.

"Corporations are completely dependent on a patchwork of software from a variety of vendors. Malware such as the keyloggers installed through browsers provide hackers access to 'secure web apps' by recording -- and later impersonating -- user actions on public websites."

What to do right now

It's a serious problem, but there are steps you can take.

Chris Gervais, vice president of engineering at cloud security and compliance company Threat Stack, told CSO that companies should take some immediate actions. Surprisingly, while Slack and Convo both offer two-factor authentication (users must verify their identity after receiving a code on their phone, for example), many companies don't use it. Enabling it creates a tighter circle of control over leaked information among registered users.

Gervais says companies can also set a custom retention period for files so that they are not available once they

are shared within the collaborative environment. Many group chat tools like HipChat allow you to set how long a chat is available in history as well. It’s also crucial to monitor (or even outright block) which bots can be added.

In Slack, he says there is a potential threat with third-party Slackbots sharing information from a company without your consent. He says you also need to audit registered users, restrict access (you might decide not to allow any contractors to access Slack, for example), and upgrade to the standard pricing plan so you can enable OAuth to control user provisioning.

“As with enterprise cloud security, visibility is key to helping secure Slack and similar collaborative tools,” he says. “Make sure you know who you're giving access to and what rights you're giving to people outside your organization.”

Another approach is more radical. Anurag Lal, CEO and president of Infinite Convergence Solutions, an enterprise chat tool, says larger companies really shouldn't be using these free and consumer-oriented chat apps. He says Slack in particular started as a gaming chat tool, and it doesn't scale well when used with thousands of users in terms of existing security infrastructure, file encryption, or even best business practices.

That’s a major step, and one that could cause a user revolt. Slack, Convo, HipChat, and many others do provide an exceptional value in terms of business process and productivity. They trump the delays and overload caused by email. Yet, anyone who decides to deploy these apps, which are free to use initially, should mitigate against the threat they pose.